LC King AIG-IT Audit

COPING WITH CYBERSECURITY

Department of Transportation OIG, 9/4/18

AGENDA

- Why another Cybersecurity Presentation?
- What’s New?
- What’s Newer & Gaining Traction?
- Why is Compliance a Bad Word?
- How Do I Determine Cybersecurity Effectiveness?
- Questions

LC King AIG-IT Audit

Why Another Cybersec Presentation?

- *Cybersecurity*: The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
- Federal Government vs. Private Sector

OPM Data Breach

CHINA'S US NAVY HACK

SHADOW BROKERS' LEAK

Snowden Leaks

Russian US Power Grid Instrusion

LC King AIG-IT Audit

What’s New

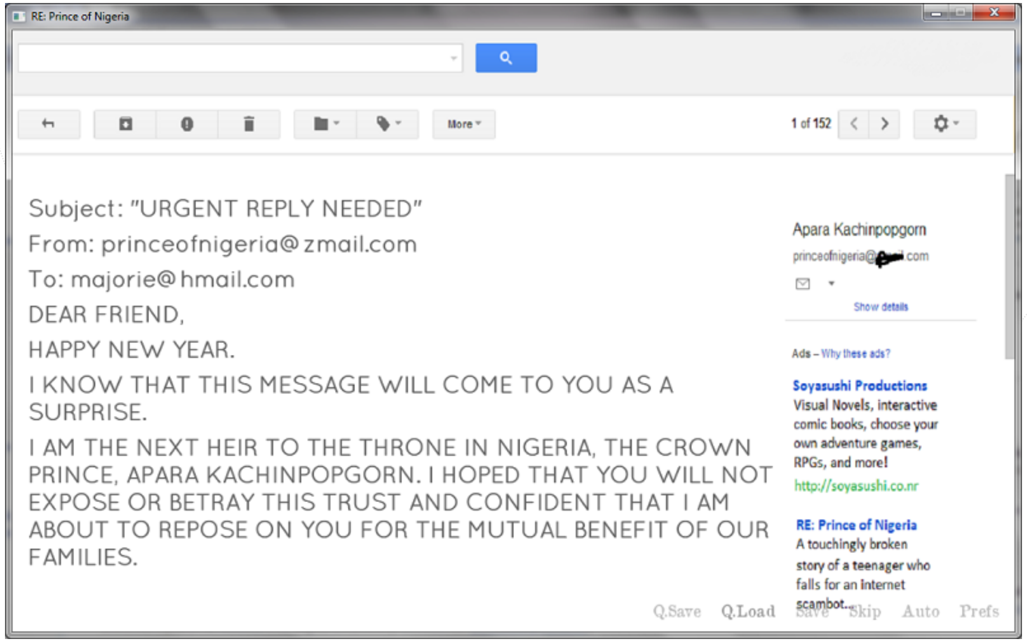
Updates to items that are now entrenched

LC King AIG-IT Audit

Social Engineering

20 YEARS AGO

TODAY



Subject: "URGENT REPLY NEEDED"
From: princeofnigeria@zmail.com
To: majorie@hmail.com

DEAR FRIEND,

HAPPY NEW YEAR.

I KNOW THAT THIS MESSAGE WILL COME TO YOU AS A SURPRISE.

I AM THE NEXT HEIR TO THE THRONE IN NIGERIA, THE CROWN PRINCE, APARA KACHINPOPGORN. I HOPED THAT YOU WILL NOT EXPOSE OR BETRAY THIS TRUST AND CONFIDENT THAT I AM ABOUT TO REPOSE ON YOU FOR THE MUTUAL BENEFIT OF OUR FAMILIES.

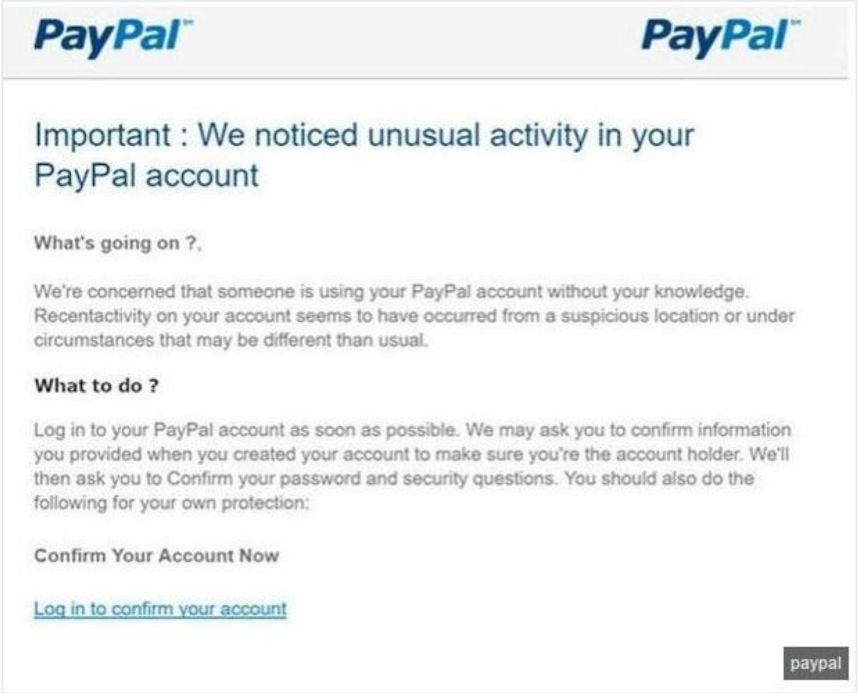
Apara Kachinpopgorn
princeofnigeria@[redacted].com

Show details

Ads – Why these ads?

Soyasushi Productions
Visual Novels, interactive comic books, choose your own adventure games, RPGs, and more!
http://soyasushi.co.nr

RE: Prince of Nigeria
A touchingly broken story of a teenager who falls for an internet scambot...



Important : We noticed unusual activity in your PayPal account

What's going on ?,

We're concerned that someone is using your PayPal account without your knowledge. Recentactivity on your account seems to have occurred from a suspicious location or under circumstances that may be different than usual.

What to do ?

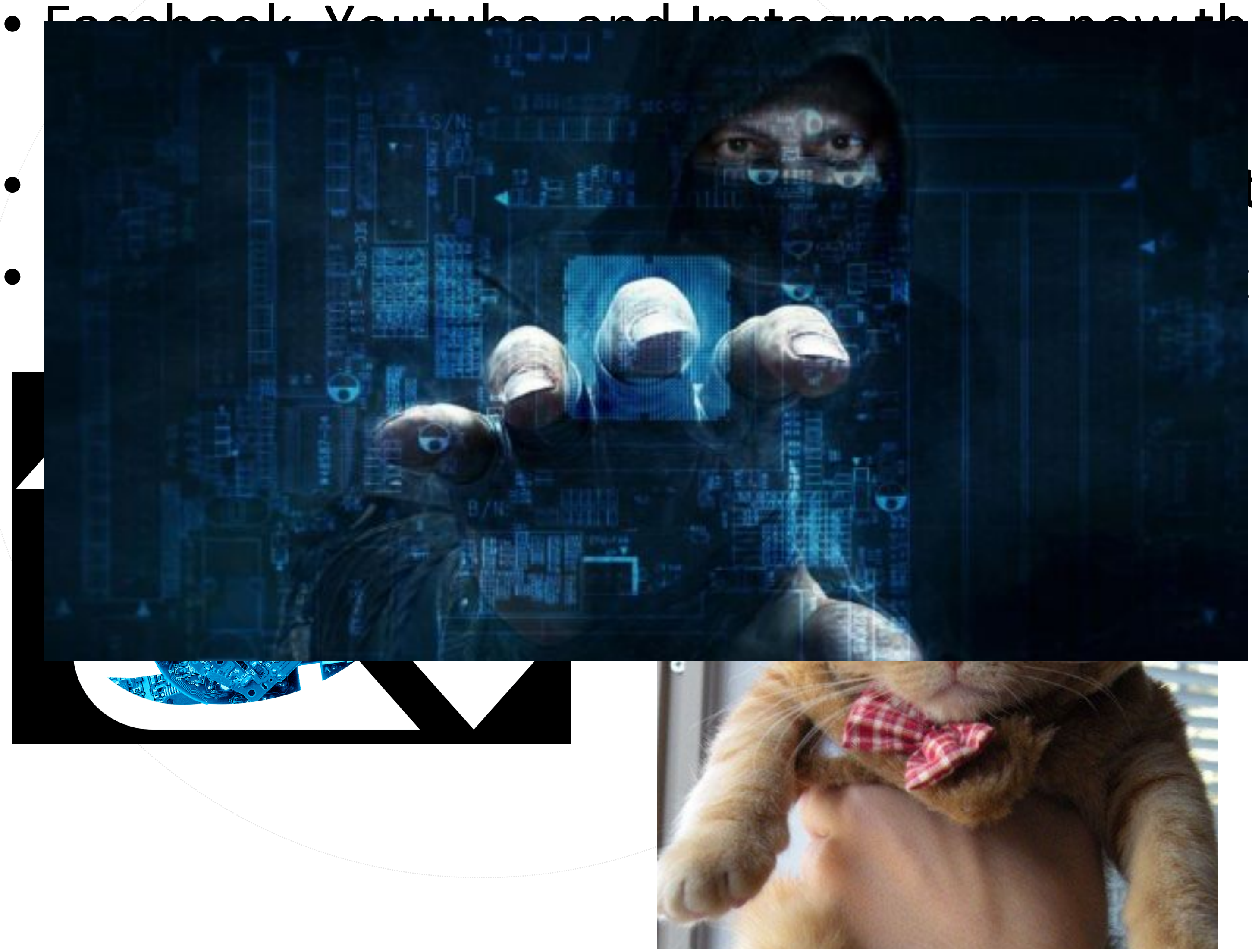
Log in to your PayPal account as soon as possible. We may ask you to confirm information you provided when you created your account to make sure you're the account holder. We'll then ask you to Confirm your password and security questions. You should also do the following for your own protection:

Confirm Your Account Now

Log in to confirm your account

SOCIAL MEDIA

- Facebook, Youtube, and Instagram are now the biggest social
- together.
- o?

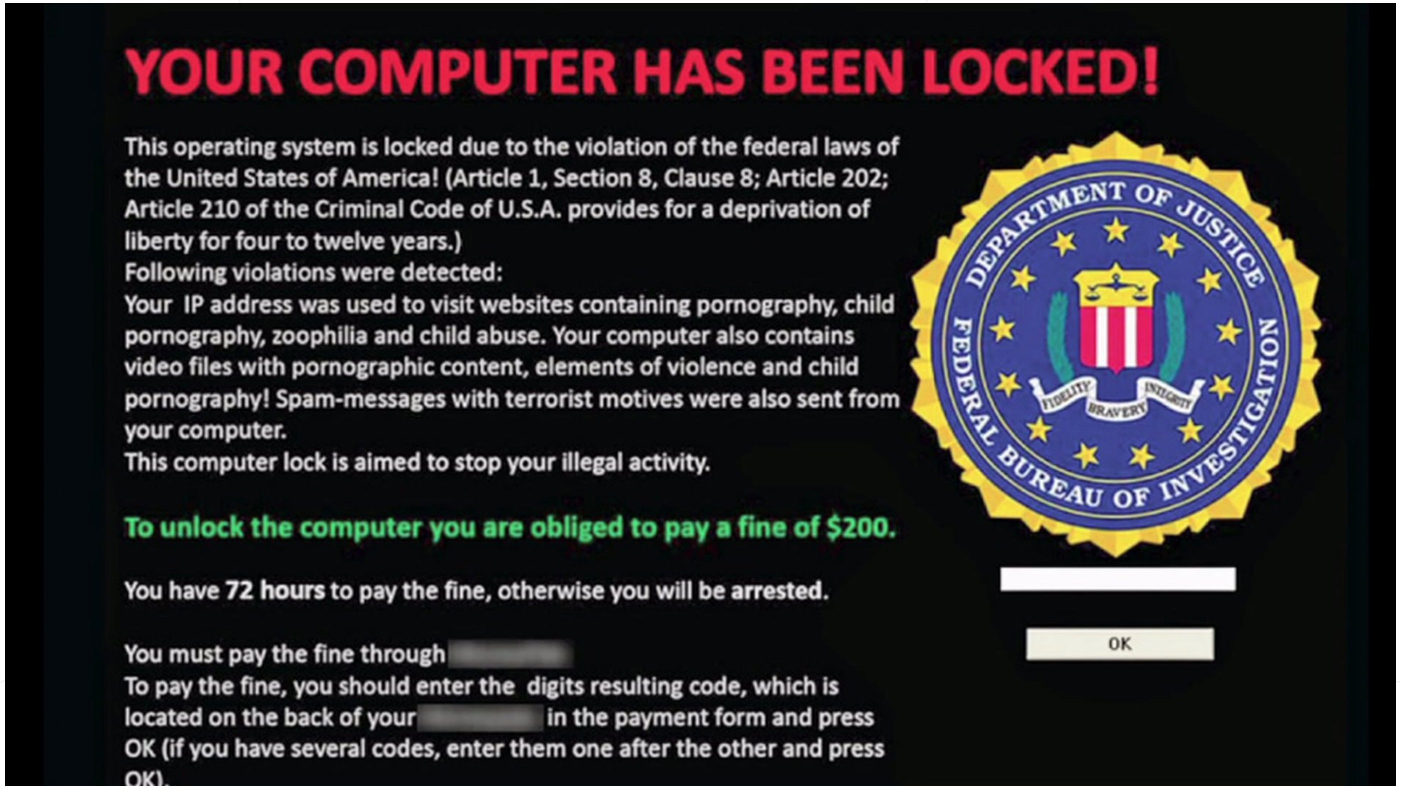


The dissemination of misinformation.

LC King AIG-IT Audit

Other Updates

- Ransomware: Wannacry attack affected over 100,000 organizations in 150 countries. Biggest online extortion attack on record affecting even hospitals.
- Crime as a Service (CAAS)
- Cryptocurrency Hacks
  - WannaMine
- Cyber Extortion
  - Clearances



YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)
Following violations were detected:
Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.
This computer lock is aimed to stop your illegal activity.

To unlock the computer you are obliged to pay a fine of $200.

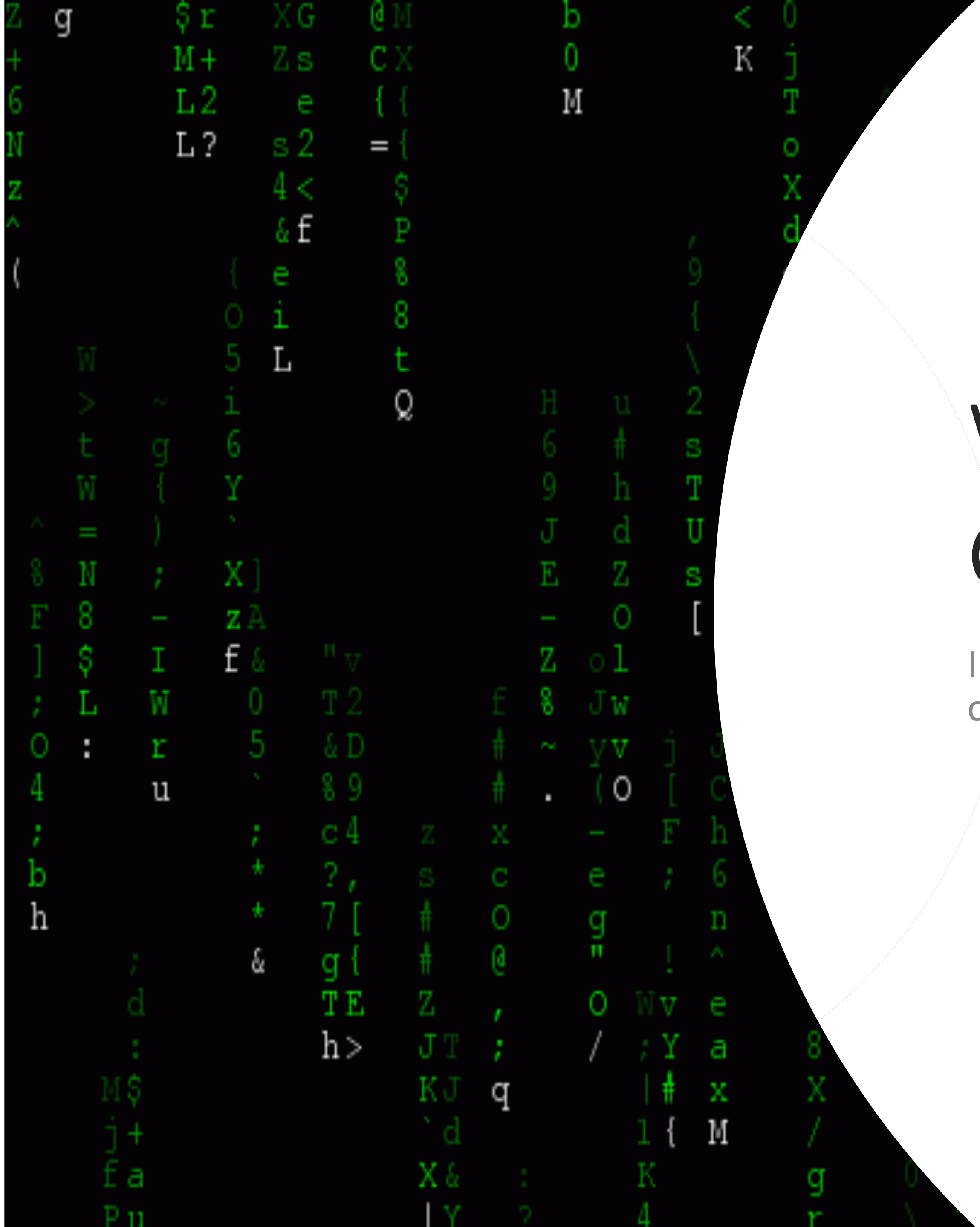
You have **72 hours** to pay the fine, otherwise you will be arrested.

You must pay the fine through [redacted]
To pay the fine, you should enter the digits resulting code, which is located on the back of your [redacted] in the payment form and press OK (if you have several codes, enter them one after the other and press OK).

ILLUSTRATION: Potential Cyber Extortion

Exercise: The Marshmallow Challenge
In 18 minutes, build the tallest free-standing structure out of 20 sticks of spaghetti, o
Cooperating

Exercise: The Marshmallow Challenge
In 18 minutes, build the tallest free-standing structure out of 20 sticks of spaghetti, o
Cooperating



What’s Newer & Gaining Traction

Items that are becoming cybersecurity concerns.

LC King AIG-IT Audit

Internet of Things

NO PRIVACY LEFT—DEVICES CAN HEAR YOU, SEE YOU, TRACK YOU AND HACK YOU

HACKABLE—CAN WEAKEN NETWORK SECURITY

MAY HAVE AUDIT USES (E.G., PENTESTS)

ARTIFICIAL INTELLIGENCE

- Progress
- Computing Power not growing as quickly as expected (2x every 18 months)

Why is Compliance a Bad Word?

The move toward maturity and effectiveness

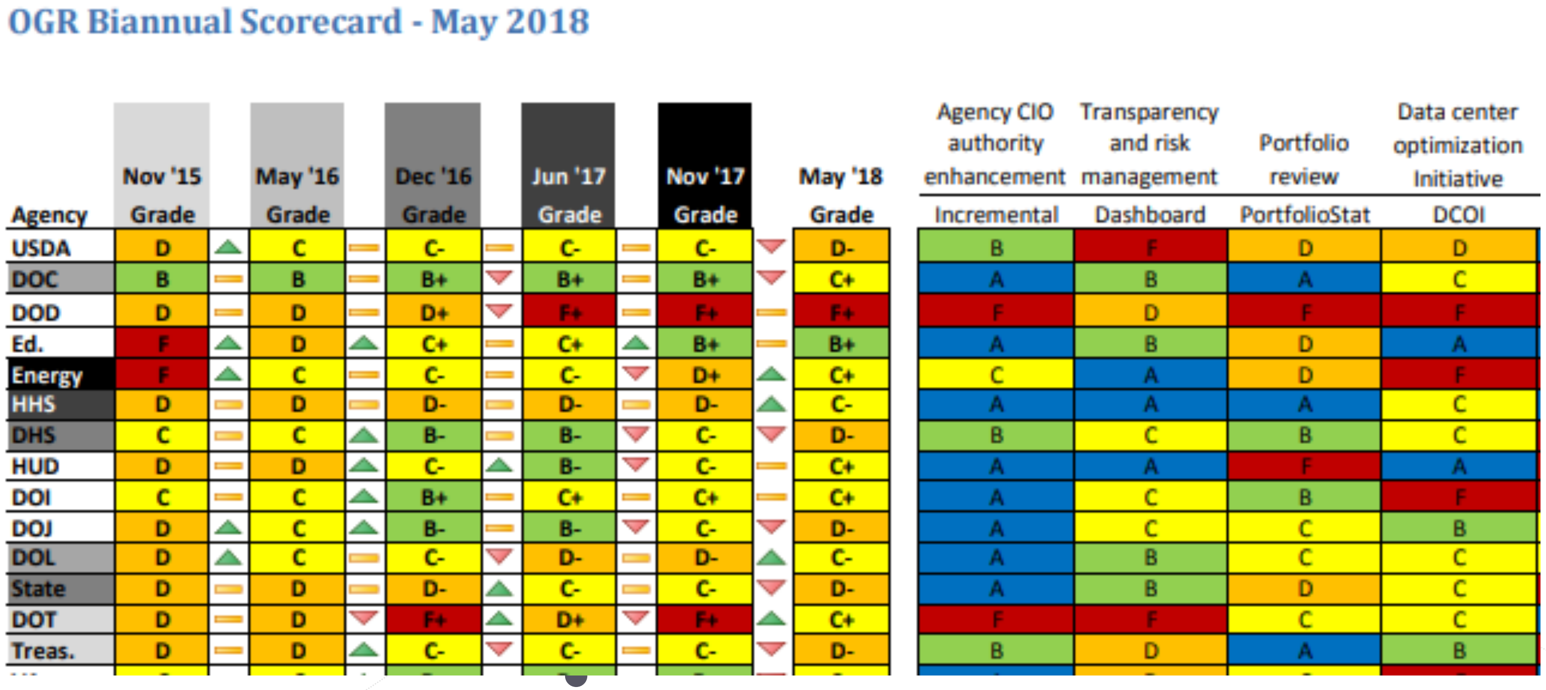
History of FISMA requirements and Scoring

1. In 2004, Rep. Adam Putnam wanted to hold agency officials accountable for their performance under the Federal Information Security Management Act (FISMA). Putnam, then chair of the House Government Reform Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, held hearings on the results of the first year under FISMA . The subcommittee in December gave the government an overall grade of D based on FISMA reports for 2003.
2. Scoring was actually done by GAO using OIG responses to OMB questions. Many of the questions were compliance oriented. For example, what percentage of employees have been trained?
3. Using scores of A, B, C, D and F was done to make the results transparent to the American public.
4. Many different parties began to make a case that an agency could be **compliant**, but not have an **effective** program.
5. OMB eliminated the use of the A, B, C, D and F scoring, favoring a more narrative based system.
6. OMB, DHS and CIGIE developed a maturity based model to assess agency effectiveness. This was a necessary change.
7. HOWEVER, What happens to an agency has not performed well in *compliance based* reviews when they move to *maturity/effectiveness based ones?* What are the side effects of changing models and metrics over a period of several years?

LC King AIG-IT Audit

FITARA 6.0 (sans Cybersecurity)

- Federal Information Technology Acquisition and Reform Act
- Biannual Scorecards prepared by House OGR with help from GAO
- Inclusion of Cybersecurity announced for next Scorecard



OGR Biannual Scorecard - May 2018

Agency	Nov '15 Grade		May '16 Grade		Dec '16 Grade		Jun '17 Grade		Nov '17 Grade		May '18 Grade	Agency CIO authority enhancement	Transparency and risk management	Portfolio review	Data center optimization Initiative
												Incremental	Dashboard	PortfolioStat	DCOI
USDA	D	▲	C	▬	C-	▬	C-	▬	C-	▼	D-	B	F	D	D
DOC	B	▬	B	▬	B+	▼	B+	▬	B+	▼	C+	A	B	A	C
DOD	D	▬	D	▬	D+	▼	F+	▬	F+	▬	F+	F	D	F	F
Ed.	F	▲	D	▲	C+	▬	C+	▲	B+	▬	B+	A	B	D	A
Energy	F	▲	C	▬	C-	▬	C-	▼	D+	▲	C+	C	A	D	F
HHS	D	▬	D	▬	D-	▬	D-	▬	D-	▲	C-	A	A	A	C
DHS	C	▬	C	▲	B-	▬	B-	▼	C-	▼	D-	B	C	B	C
HUD	D	▬	D	▲	C-	▲	B-	▼	C-	▬	C+	A	A	F	A
DOI	C	▬	C	▲	B+	▬	C+	▬	C+	▬	C+	A	C	B	F
DOJ	D	▲	C	▲	B-	▬	B-	▼	C-	▼	D-	A	C	C	B
DOL	D	▲	C	▬	C-	▼	D-	▬	D-	▲	C-	A	B	C	C
State	D	▬	D	▬	D-	▲	C-	▬	C-	▼	D-	A	B	D	C
DOT	D	▬	D	▼	F+	▲	D+	▼	F+	▲	C+	F	F	C	C
Treas.	D	▬	D	▲	C-	▼	C-	▬	C-	▼	D-	B	D	A	B

LC King AIG-IT Audit

How do I identify cybersecurity effectiveness?

IE, how do I begin to meet FISMA review requirements?

EXAMPLE: Reviewing Security Awareness Training

RESEARCH	RESULTS Pt. 1	RESULTS Pt. 2	COMMENTS
Are there statutory requirements?	Yes—FISMA mandates a program.	Serves as criteria to mandate the overall program.	Without a program, the agency has a statutory noncompliance.
Are there relevant NIST publications?	Yes. NIST 800-50 provides guidance.	Useful for criteria—agency may argue it is not required.	**Criteria does not have to be a requirement**.
Are there relevant OMB or DHS issuances?	OMB A-130 requires a program consistent with NIST.	Useful for criteria.	See above.
Does the agency provide training to employees?	If Yes, proceed.	It is probably to early to reach a conclusion.	Compliance step. However, if you don't comply, you can't be effective.
Does the agency track training?	If Yes and percentage trained is reasonable, proceed.	If no, Agency cannot demonstrate effectiveness. You have option of testing to develop percentage.	Compliance tracking step. Without it, you can't assess effectiveness.
Does the agency evaluate content of training?	If Yes, proceed.	*Training must have appropriate content to be effective.*	***Move from compliance to effectiveness*** *by adding review of quality of training.*
Does the agency perform tests to assess actual learning?	If Yes, proceed.	*Further supports effectiveness.*	*Effectiveness test that can be measured. Auditor can perform separately.*
Does the agency use tests to improve program?	If yes, you may be done.	*Agency is likely effective.*	*Judgement call if you need to test this. You may already have concluded agency is effective.*

Problem Areas

- RISK
  - Risk Tolerance
  - RISK ACCEPTANCE
- Transition from 3 Year to Ongoing System Authorization
  - Gap on how to stay secure during transition
  - Execution strategies are not clear
- Shared/Inherited Controls (large organizations)
  - Which ones?
  - Is status properly communicated?
  - What happens when provider fails to provide control? How should mitigation be handled?
- Stagnation—What is the cause?

Leaves Hands Feeling Soft & Refreshed
with Moisturizers & Vitamin E
Purell
HAND SANITIZER
Kills 99.99% of Germs
8 FL OZ (236 mL)

Example: Problem Areas

- Central Operating Network (CON) supports HQ and 11 components.
- All components’ networks inherit controls.
- Controls tested December 2014 and March 2018. No annual testing.
- Implementation of network scanning software only partially successful in past.
- Current testing showed many of the same common control failures found in December 2014.
- Components believe they are limited as to implementation of mitigating controls partially due to FITARA.
- Communicating issues to senior management is difficult due technical nature of issues.
- Agency position is that Authorizing Official of the CON can assume risk for the network and components.
- Agency further believes that its risk acceptance cannot be questioned by the OIG. Once the Authorizing Official accepts risk, control weaknesses are deemed acceptable.
- ***Do you agree?***

QUESTIONS

Thank You!

👤 Louis C. King

📱 +1 202 366 1407

✉ Louis.King@oig.dot.gov